This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Canceled)

2. (Canceled)

3. (Currently Amended) A method of detecting surveillance probes on a computer communications network, comprising:

receiving a plurality of messages from a data sensor, located at a network audit point, that samples data packets on said computer communications network and outputs said messages, each of said messages describing an event occurring on said communications network;

processing said messages to form extrapolated connection sessions from said sampled data packets by clustering packets a) exchanged between two addresses within a specified time period where the addresses are not predetermined or (b) having certain flags set or c) having addresses that are not predetermined but have similar characteristics; and

detecting a surveillance probe by:

grouping connection sessions into a plurality of groups;

scoring each group; and

generating an alert for each group whose score is greater than an empirically derived threshold.

4. (Canceled)

5. (Previously Presented) The method of claim 3, further comprising controlling false positive detections vs. false negative detections.

6. (Currently Amended) The method of claim 3, further comprising generating a profile of surveillance activity, said profile of surveillance activity comprising one or more of the following:

a breakdown of probes;

a number of attackers;

a number of attacks per unit time;

a percentage of activity that constitutes malicious surveillance;

a breakdown of source country frequencies;

the most frequently-targeted network addresses; and

[[a]] temporal frequency trends of individual attackers.

7. (Currently Amended) The method of claim 3, further comprising processing one or more of said detected surveillance probes to produce a detected surveillance scan, said processing of one or more of said detected surveillance probes to produce a detected surveillance scan comprising one or more of the following:

modeling and detecting surveillance scans as a series of surveillance probes that originate from one or more source addresses and that are sent to one or more destination addresses;

modeling and detecting surveillance scans performed by a particular source address by identifying a particular source address that sends more than a specified number of probes;

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that generates more than a specified number of probes within a specified time period;

modeling and detecting surveillance scans performed by one source IP address by identifying a source address that sends probes to more than a specified number of destinations;

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that sends probes to a specified set of destinations;

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that sends probes to specified ports; and

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that sends probes to a number of destinations in excess of a specified limit within a specified time period.

8. (Previously Presented) The method of claim 7, further comprising controlling false positive detections vs. false negative detections.

9. (Currently Amended) The method of claim 7, further comprising generating a profile of surveillance activity, said profile of surveillance activity comprising one or more of the following:

a breakdown of probes;

a breakdown of scans;

a number of attackers;

a number of attacks per unit time;

a percentage of activity that constitutes malicious surveillance;

a breakdown of source country frequencies;

the most frequently-targeted network addresses; and

[[a]] temporal frequency trends of individual attackers.

10. (Currently Amended) The method of claim 7, further comprising processing one or more of said detected surveillance scans to detect a group of scanning hosts, said processing of one or more of said detected surveillance scans to detect a group of scanning hosts comprising:

modeling and detecting scans distributed across a series of source addresses by grouping addresses, said grouping of addresses being performed by subtracting one address from another and placing the two addresses in the same group if the difference is less than a specified amount.

11. (Previously Presented) The method of claim 10, further comprising controlling false positive detections vs. false negative detections.

12. (Currently Amended) The method of claim 10, further comprising generating a profile of surveillance activity, said profile of surveillance activity comprising one or more of the following:

a breakdown of probes;

a breakdown of scans;

a number of attackers;

a number of attacks per unit time;

a percentage of activity that constitutes malicious surveillance;

a breakdown of source country frequencies;

the most frequently-targeted network addresses; and

[[a]] temporal frequency trends of individual attackers.

13. (Canceled)

14. (Canceled)

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Currently Amended) The method of claim 3 wherein the step of processing said messages to form extrapolated connection sessions ~~to detect~~ and detecting a surveillance probe further comprises at least one of the following steps:

identifying packets that have a particular arrangement of flags set;

identifying packets that have all flags set;

identifying packets that have payloads smaller than a predetermined size;

identifying packets to which there is no response.

20. (Currently Amended) The method of claim 3 wherein the steps of processing said messages to form extrapolated connection sessions ~~to detect~~ and detecting a surveillance probe further comprises at least one of the following steps:

identifying detected connections with fewer packets than a predetermined limit;

identifying detected connections with packets that have traveled only from a source to a destination;

identifying detected connections with packets that have traveled only from the destination to the source; and

identifying detected connections with packets whose payloads are smaller than a predetermined limit

21. (Previously Presented) The method of claim 7 further comprising the steps of:

limiting the number of detected scans by reporting only source addresses that perform more than a specified number of probes within a specified time; and

limiting the number of detected scans by reporting only source address groups that perform more than a specified number of probes within a specified time.

22. (New) A system for detecting surveillance probes on a computer communications network, comprising:

a data sensor located at a network audit point adapted to sample data packets on said computer communications network and to output messages, each of said messages describing an event occurring on said communications network; and

a processor that processes said messages to form extrapolated connection sessions from said sampled data packets by clustering packets a) exchanged between two addresses within a specified time period where the addresses are not predetermined or (b) having certain flags set or c) having addresses that are not predetermined but have similar characteristics, and that detects a surveillance probe by grouping connection sessions into a plurality of groups, scoring each group, and generating an alert for each group whose score is greater than an empirically derived threshold.

23. (New) The system of claim 22, wherein said processor further generates a profile of surveillance activity comprising one or more of the following:

a breakdown of probes;

a number of attackers;

a number of attacks per unit time;

a percentage of activity that constitutes malicious surveillance;

a breakdown of source country frequencies;

the most frequently-targeted network addresses; and

temporal frequency trends of individual attackers.

24. (New) The system of claim 22, wherein said processor further processes one or more of said detected surveillance probes to produce a detected surveillance scan by performing one or more of the following steps:

modeling and detecting surveillance scans as a series of surveillance probes that originate from one or more source addresses and that are sent to one or more destination addresses;

modeling and detecting surveillance scans performed by a particular source address by identifying a particular source address that sends more than a specified number of probes;

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that generates more than a specified number of probes within a specified time period;

modeling and detecting surveillance scans performed by one source IP address by identifying a source address that sends probes to more than a specified number of destinations;

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that sends probes to a specified set of destinations;

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that sends probes to specified ports; and

modeling and detecting surveillance scans performed by a particular source address by identifying a source address that sends probes to a number of destinations in excess of a specified limit within a specified time period.

25. (New) The system of claim 24, wherein said processor further processes one or more of said detected surveillance scans to detect a group of scanning hosts by modeling and detecting scans distributed across a series of source addresses by grouping addresses, said

grouping of addresses being performed by subtracting one address from another and placing the two addresses in the same group if the difference is less than a specified amount.

26. (New) The system of claim 22 wherein the processor is also programmed to perform at least one of the following steps:

identifying packets that have a particular arrangement of flags set;

identifying packets that have all flags set;

identifying packets that have payloads smaller than a predetermined size;

identifying packets to which there is no response.

27. (New) The system of claim 22 wherein the processor is further programmed to perform at least one of the following steps:

identifying detected connections with fewer packets than a predetermined limit;

identifying detected connections with packets that have traveled only from a source to a destination;

identifying detected connections with packets that have traveled only from the destination to the source; and

identifying detected connections with packets whose payloads are smaller than a predetermined limit

28. (New) The system of claim 24 wherein the processor is further programmed to perform the steps of:

limiting the number of detected scans by reporting only source addresses that perform more than a specified number of probes within a specified time; and

limiting the number of detected scans by reporting only source address groups that perform more than a specified number of probes within a specified time.